UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

United States of America,

Plaintiff,

v.

Michael Robert Granley.

Defendant.

Court File No. 16-cr-196 (ADM/LIB)

REPORT AND RECOMMENDATION

This matter came before the undersigned United States Magistrate Judge pursuant to a general assignment, made in accordance with the provisions of 28 U.S.C. § 636 and Local Rule 72.1, and upon Defendant's Motion to Suppress Evidence Obtained as a Result of Search and Seizure, [Docket No. 31]. The Court held a motions hearing on September 30, 2016, regarding the parties' pretrial motions.[1]

At the motions hearing, the parties requested the opportunity to submit supplemental briefing, which was completed on October 19, 2016, and after which the Defendant's Motion to Suppress, [Docket No. 31], was taken under advisement by the undersigned. For the reasons set forth below, the Court recommends that Defendants' Motion to Suppress Evidence Obtained as a Result of Search and Seizure, [Docket No. 31], be **DENIED**.

I. RELEVANT FACTS

On January 14, 2016, Investigator Chris Benson with the Clearwater County Sheriff's Office received a report from the Waynesboro, Virginia, Police Department of an online conversation between a 12-year-old female, H.F., and "Michael Granley," an approximately 42-

[1] The Court addressed the parties' pretrial discovery motions by separate order. ([Docket No. 38]).

year-old male. (Govt. Exh. 3, [Docket No. 34-3], 3-4). H.F.'s sister, C.W., had shown screenshots of the conversation to the Waynesboro Police Department's School Resource Officer, Officer Layman. (Id. at 4). The report from Officer Layman described a "sexually charged conversation" in which "Michael Granley" told H.F. that she was attractive; acknowledged twice that H.F. was 13 years old and told her they would "have to be careful because of our age"; told H.F. that "guys have 2 heads" and asked her twice which head she wanted to see; asked H.F. if she knew what a clit is; told her that girls have two lips and asked H.F. which lips she wanted him to kiss; told her he was "about 7 inches long down there"; suggested meeting in a hotel room to play video games, during which he might accidentally "touch her boobs"; told her that if they met he would "give [her] his dick"; talked about going to a hotel room together to change clothes; and suggested that H.F. get into a hotel hot tub to watch movies. (Id.). After reviewing the report, Investigator Benson spoke with Detective Dunn of the Waynesboro Police Department, who informed Investigator Benson that he had investigated the matter and discovered that the IP address used in the online conversation was registered in Clearwater County. (Id.).

Investigator Benson also received a report from the Bemidji Police Department of a Michael Granley who had had an online conversation with J.G., a juvenile female. (Id.). The Bemidji Police Department gave Investigator Benson a screenshot of a conversation in which Michael Granley requested a picture of J.G.'s "boobs," then said, "[N]ot gonna ask for the other thing. Ur only 12. . . . unless you want to send a pussy pic." (Id.).

Investigator Benson noted that the profile image used by Michael Granley in both conversations was the same. (Id.). Thus, Investigator Benson drafted an administrative subpoena to obtain the subscriber information for the IP address, which was registered with Garden Valley

Telephone Company of Erskine, Minnesota. (Id.). Pursuant to the subpoena, Garden Valley Telephone Company identified the IP address subscriber as Robert Granley and provided a physical address for the IP address. (Id.). When Investigator Benson ran a Minnesota driver's license check, he discovered that Defendant Michael Granley's ("Defendant") listed address was the same as the physical address for the IP address. (Id.).

Investigator Benson called Robert Granley and asked to speak with Defendant. Defendant was not home, but Investigator Benson learned that Defendant lived at the residence full-time with his parents, Robert and Sandy Granley. (Id.). Investigator Benson then searched for a Facebook account in Defendant's name and, although he found a Facebook page that a Michael Granley had liked, he could not locate a Facebook account in Defendant's name. (Id.).

As a result, on January 19, 2016, Investigator Benson applied for a search warrant to search Defendant's home and his person. (Id. at 3-5). The affidavit in support of the search warrant application contained the information related above and related that Investigator Benson knew "that an electronic device connected to the internet via wireless or hard wire is needed to access and maintain the Facebook page." (Id.). Therefore, Investigator Benson "request[ed] a search warrant to access the electronic devices maintained and/or utilized by [Defendant] for the purpose of maintaining and/or collecting of photographs of children for either personal gratification or trade." (Id. at 5).

State court Judge John Melbye signed the search warrant, authorizing a search of the residence and Defendant's person for:

1. Computer system including, but not limited to: the main computer box, central processing units, hard drives, monitors, scanners, printers, modems and/or other peripheral devices;
2. Media in whatever form, including but not limited to be magnetic (i.e. floppy disks and tapes), optical (i.e. CD's and DVD's), and/or solid state (i.e. Flash Drives and Memory Cards);

3. Personal electronic devices including, but not limited to: cell phones, personal data assistants, portable audio devices, digital cameras, digital video recorders, video entertainment consoles, and/or any other data storage medium;
4. Data contained on either hard drives or removable media to include: deleted files and e-mail files that may show the receipt, possession, and/or distribution of child pornography; chat line logs that may identify children being enticed online; or data that reveals the distribution of child pornography;
5. Papers and effects that tend to show the possession or distribution of child pornography or the enticement of children online, including but not limited to address books or diaries;
6. Notes and other documentation that may reveal logins and or passwords;
7. Programs and manuals relating to the operating systems or any applications;
8. Proof of residency and documentation relating to the internet including but not limited to bills from the internet service provider;
9. Any and all camera equipment, videotapes, or other items that may be used for the possession, production, and/or distribution of child pornography;
10. Depictions of minors under the age of eighteen engaged in or simulating prohibited sexual acts, such as: actual or simulated sexual intercourse, deviant sexual intercourse, sadism, masochism, sexual bestiality, incest, masturbation, or sadomasochistic abuse; actual or simulated exhibition of the genitals, the pubic or rectal area, or the bare feminine breasts, in a lewd or lascivious manner; actual physical contact with a person's clothed or unclothed genitals, pubic area, buttocks, or if such a person is female, breast with the intent to arouse or gratify the sexual desire of either party; defecation or urination for the purpose of creating sexual excitement in the view; and/or any act or conduct which constitutes a Criminal Sexual Assault or simulates that a Criminal Sexual Assault is being or will be committed.;
11. Depictions of nudity involving minors under the age of 18 years of age; showing or the simulated showing of the human male or female genitals, pubic area, or buttocks with less than a fully opaque covering; showing of the female breast with less than a fully opaque covering of any portion thereof below the top of the nipple; and/or the depiction of the covered male genitals in a discernibly turgid state for the purpose of creating sexual excitement;
12. Any evidence related to the sexual exploitation of children
13. Authority to photograph the above-described items and their location within the premises;
14. Authority to seize and transport for examination by persons qualified to do so, and in a laboratory setting, any and all electronic data processing and computer storage devices at an offsite location, Bureau of Criminal Apprehension (BCA).

(Id. at 6-7).

On January 20, 2016, Investigator Benson executed the search warrant at Defendant's home, but did not seize anything. (September 30, 2016, Motions Hearing, Digital Record, 2:08-09, 2:12-13). Defendant's parents were home at the time, but Defendant was not. Defendant's parents told Investigator Benson that Defendant would be spending the night in Park Rapids, Minnesota. (Id. at 2:12-14).

The next day, local law enforcement in Park Rapids informed Investigator Benson that they had located Defendant's vehicle at a real estate office. (Id.). While Investigator Benson was driving to Park Rapids, law enforcement called again and said that it appeared that Defendant was attempting to leave; at Investigator Benson's request, local law enforcement temporarily detained Defendant to wait for Investigator Benson. (Id. at 2:14-15). When Investigator Benson arrived at the real estate office, Defendant agreed to talk with him. (Id. at 2:09-10).

They went into an office, where Defendant informed Investigator Benson that he had spoken with his father, who had advised him to give up his electronic devices. (Id.). Investigator Benson told Defendant why he was there and showed him a copy of the search warrant. (Id. at 2:15-17). At that point, Defendant gave Investigator Benson his iPhone and, after retrieving his tablet from his luggage, gave Investigator Benson the tablet, too. (Id. at 2:09-:11, 2:20-21). Investigator Benson gave Defendant a receipt for the items and took them to the BCA, where they were forensically examined. [2] (Id. at 2:10-11).

The forensic examination of the iPhone and tablet revealed several additional conversations with underage females. (Govt. Exh. 2, [Docket No. 34-2], 4). In an online conversation with a 14-year-old girl, K.C., Defendant requested a photograph of K.C.'s "boobs," sent K.C. a photograph of a penis, told K.C. that she needed to delete the messages, and talked

[2] Although it is undisputed that Investigator Benson did not promptly file an inventory return, (September 30, 2016, Motions Hearing, Digital Record, 2:16-19), the Court notes that Benson filed an inventory return on October 4, 2016, recording the seizure of the cell phone and tablet. (Govt. Exh. A, [Docket No. 42-1]).

with K.C. about the two of them "having a threesome" with another person. (Govt. Exh. 2, [Docket No. 34-2], 4). During a conversation with K.C., Defendant received photographs of female breasts. (Id.).

By locating K.C. on Facebook, Investigator Benson found that K.C. was possibly from the Bellefontaine, Ohio, area, so he requested assistance from Detective Sebring of the Bellefontaine Police Department in locating K.C. (Id.). Similarly, Investigator Benson began trying to identify and locate several other females related to information found on Defendant's iPhone. (Id.). Data on the iPhone also showed that Defendant had deactivated his Facebook account but subsequently had tried to reactivate it. (Id. at 5) In addition, there was an active iCloud account associated with the phone, which Investigator Benson knew could be used to store and share saved images, documents, notes, contacts, and locations. (Id.)

Based on the information from the forensic examination of the iPhone, on January 27, 2016, Investigator Benson sought three additional search warrants. The first was a search warrant for the iCloud account "for images related to the solicitation of children for personal gratification or trade." (Id.). The affidavit in support of the application for a search warrant included the information detailed above. (Id. at 3-5). State court judge Robert D. Tiffany signed the search warrant on January 27, 2016, authorizing a search of

1. Any and all information for iCloud email account granley24@gmail.com to include name and address; alternate email addresses; passwords; IP addresses; date and time of registration; account status; and log-in IP addresses associated with session times and dates; from the date of the account creation to present date.
2. For the subscriber identified as granley24@gmail.com the contents of any and all emails sent or received, to include full header information and all attachments, stored in the subscriber's iCloud account; from the date of account creation to present date.
3. Any and all contents of electronic files that subscriber granley24@gmail.com has stored in the subscriber's email account to include saved/sent/deleted/and

> any other folder associated with this email account; from the date of account creation to present date.

(Id. at 6).

The second search warrant Investigator Benson applied for sought information from Defendant's Facebook Account, "to verify if there was communication or any additional requests for photographs involving nude or sexually explicit females to include juvenile females." (Govt. Exh. 4, [Docket No. 34-4], 5). In the affidavit in support of the application for this search warrant, Investigator Benson related the information detailed above and explained some of the features of Facebook, the basic contact information Facebook requires of its users, and the records Facebook retains regarding its users' communications and data. (Id. at 5-7).

Judge Tiffany signed this search warrant as well, authorizing a search for:

1. All contact information for user ID: https://www.facebook.com/michael.granley.7, email address: granley24@gmail.com, including full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
2. All Photoprints, including all photos uploaded by user ID: https://www.facebook.com/michael.granley.7, email address: granley24@gmail.com and all photos uploaded by any user that have that user tagged in them;
3. All Neoprints, including profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
4. All other communications and messages made or received by the user, including all private messages and pending "Friend" requests;
5. All IP logs, including all records of the IP addresses that logged into the account;
6. All information about the user's access and use of Facebook Marketplace;
7. The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);

8. All privacy settings and other account settings;
9. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.
10. All information which constitutes fruits, evidence and instrumentalities of violations of MN Statute 617.247.4(a), involving female minors since June 1, 2015, including each user ID and information pertaining to the following matters: Possession of Pornographic Work Involving Minors;
11. Records relating to who created, used, or communicated with user ID: https://www.facebook.com/michael.granley.7, email address: granley24@gmail.com, including records about their identities and whereabouts.

(Id. at 8-9).

The third search warrant for which Investigator Benson applied on January 27, 2016, was for Defendant's Google account and requested a search warrant for Google Legal Investigations Support for:

1. ANY AND ALL STORED CONTENT: Subscriber information, Picasa Web Albums, Google Chrome Sync, Google Profile, Google Wallet, Any and all past and current phone numbers associated with the listed account.
DATE RANGE SPECIFIC ITEMS: ANY Google Multilogin, Google calendar, Web history, Gmail incoming and outgoing messages, associated IP addresses, AND ALL LOCATION HISTORY associated with the listed account for time period of:
June 1 2015 at 0000 hours through January 21 2016 at 2300 hours.

(Govt. Exh. 1, [Docket No. 34-1], 2). The affidavit in support of this search warrant application included the information related above. (Id. at 2-5). Judge Tiffany signed this search warrant as well. (Id. at 7).

Through his investigation and information obtained through the search warrants, Investigator Benson discovered that Defendant had used his Facebook account to communicate with a 15-year-old female in Pennsylvania, whom he sent multiple images of an erect penis, from whom he solicited naked images, and with whom he talked about his driving to Pennsylvania to

have sex with her. (Id. at 20-21). A law enforcement agent in Pennsylvania informed Investigator Benson that Defendant had made hotel reservations near where this female lived. (Id. at 21).

After Investigator Benson spoke with Defendant, Investigator Benson could no longer find the Facebook profile under the name Michael Granley, but he did find a Facebook profile for Mike Granley, with a profile picture that matched Defendant. (Id.). In mid-February, an undercover law enforcement officer sent a friend request to this Facebook account. (Id.) In a private message, Defendant said he was in a relationship with the Pennsylvania minor and that he was planning on visiting her. (Id.). The undercover officer pretended to be a friend of the minor and mentioned that the minor was 15 years old. (Id.). Defendant did not comment on the minor's age; instead, he expressed interest in spending time with the undercover officer while he was in Pennsylvania visiting the minor. (Id. at 21-22).

On July 14, 2016, Investigator Benson applied for a fifth search warrant, this time for information related to the Mike Granley Facebook account. (Govt. Exh. 5, [Docket No. 34-5], 2, 6). The affidavit Investigator Benson submitted in support of this search warrant application related the facts set forth above, and again related general information about Facebook. (Id. at 14-20). Although the signed search warrant has not been submitted to this Court, the parties agree that the search warrant was signed and executed. (See Def.'s Mem. in Support of Motion to Suppress, [Docket No. 40], 15; Govt.'s Response to Def.'s Mem., [Docket No. 42], 21).

The Government subsequently indicted Defendant on ten counts of transferring obscene material to a minor, three counts of production of child pornography, and two counts of attempted production of child pornography. (Indictment, [Docket No. 1]).

II. DEFENDANT'S MOTION TO SUPPRESS [Docket No. 31]

Defendant moves the Court for an order suppressing the physical evidence obtained as a result of the execution of any and all of the search warrants in this case. He argues that (1) the affidavit submitted in support of the initial search warrant application did not provide probable cause to issue the warrant; (2) the warrant did not cover the seizure of the iPhone and tablet from Defendant; and (3) the search of the contents of the iPhone and tablet was illegal because neither the warrant nor the application specified the cell phone and tablet as items to be searched. (Def.'s Mem. in Support of Motion to Suppress, [Docket No. 40], 1, 10). Defendant also asks the Court to suppress the evidence obtained by execution of the subsequent warrants on the grounds that those warrants were issued based in part on information illegally obtained by execution of the first warrant and are not independently supported by probable cause. (Id. at 1).

In response, the Government asserts that the affidavit in support of the initial search warrant contained sufficient facts to establish probable cause to support the search, it was not overly broad, it authorized the seizure of the iPhone and tablet from Defendant, and there was no need to obtain a separate warrant to search the iPhone or tablet. (Govt. Response, [Docket No. 42], 8-19). In addition, the Government argues that even if the warrant in support of the application for the initial search warrant did not contain sufficient facts to establish probable cause to support the search and seizure, the evidence obtained in that search and used in the applications for the subsequent warrants is admissible because the officers executing the warrant reasonably relied on the judge's determination that there was probable cause to issue the search warrant. (Id. at 20-21). Finally, the Government asserts that even without the information discovered through the initial search warrant, there was probable cause to support the subsequent warrants. (Id. at 21-22).

A. Standards of Review

The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and that "no warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. Amend. IV. Moreover, the Fourth Amendment requires warrants to "particularly describ[e] the place to be searched, and the person or things to be seized." Id.

The Eighth Circuit has held that "[a]n affidavit establishes probable cause for a warrant if it sets forth sufficient facts to establish that there is a fair probability that contraband or evidence of criminal activity will be found in the particular place to be searched." United States v. Mutschelknaus, 592 F.3d 826, 828 (8th Cir. 2010) (internal quotation marks and citation omitted). "Probable cause is a fluid concept that focuses on 'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.'" United States v. Colbert, 605 F.3d 573, 576 (8th Cir. 2010) (quoting Illinois v. Gates, 462 U.S. 213, 231 (1983)). Courts use a "'totality of the circumstances test . . . to determine whether probable cause exists.'" United States v. Hager, 710 F.3d 830, 836 (8th Cir. 2013) (citation omitted).

The sufficiency of a search warrant affidavit is examined using "common sense and not a hypertechnical approach." United States v. Grant, 490 F.3d 627, 632 (8th Cir. 2007) (citation and internal quotations omitted). "In ruling on a motion to suppress, probable cause is determined based on 'the information before the issuing judicial officer.'" United States v. Smith, 581 F.3d 692, 694 (8th Cir. 2009) (quoting United States v. Reivich, 793 F.2d 957, 959 (8th Cir. 1986)). "Therefore, '[w]hen the [issuing judge] relied solely upon the supporting affidavit to issue the warrant, only that information which is found in the four corners of the affidavit may be

considered in determining the existence of probable cause.'" United States v. Wiley, No. 09-cr-239 (JRT/FLN), 2009 WL 5033956, at *2 (D. Minn. Dec. 15, 2009) (Tunheim, J.) (quoting United States v. Solomon, 432 F.3d 824, 827 (8th Cir. 2005); edits in Wiley).

In addition, the issuing court's "'determination of probable cause should be paid great deference by reviewing courts,'" Gates, 462 U.S. at 236 (quoting Spinelli v. United States, 393 U.S. 410, 419 (1969)). "[T]he duty of a reviewing court is simply to ensure that the issuing court] had a 'substantial basis for . . . [concluding]' that probable cause existed." Id. at 238-39 (quoting Jones v. United States, 362 U.S. 257, 271 (1960)).

B. Analysis

Defendant asserts multiple problems which he argues render the affidavit submitted in support of the initial search warrant invalid. The first series of challenges are attacks on whether the affidavit provided the requisite probable cause.

a. Probable Cause

First, Defendant claims that the statements in the affidavit that identified him as being associated with the IP address at issue were conclusory. (Def.'s Mem. in Support of Motion to Suppress, [Docket No. 40], 4).

The United States Supreme Court has explained that "[a]n affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause"; it cannot contain only "mere conclusory statement[s] that give[] the magistrate virtually no basis at all for making a judgment regarding probable cause." Gates, 462 U.S. at 239. "[W]holly conclusory statements that the affiant 'has cause to suspect and does believe that' illegal activity is occurring 'will not do.'" United States v. Tripp, 370 Fed. Appx. 753, 757 (8th Cir. 2010) (quoting Gates, 462 U.S. at 239).

Specifically, Defendant asserts that the affidavit "fails to specify how [Defendant] was identified as the source of the alleged 'online conversations,'" nor does it specify how the IP address allegedly used in the Waynesboro, Virginia, conversations was determined (Id. at 7). The Government contests these assertions, arguing that the affidavit contained detailed facts regarding the investigation and how Investigator Benson identified Defendant as the suspect. (Govt. Response, [Docket No. 42], 8-10). After review of the supporting affidavit at issue, the Court agrees with the Government.

Investigator Benson's affidavit thoroughly explains how he came to identify Defendant and associate him with the IP address: Investigator Benson received a report of a sexually charged online conversation between a person with the same name as Defendant and a 12-year-old girl in Virginia. (Govt. Exh. 3, [Docket No. 34-3], 4). The detective in Virginia who had investigated the report there informed Investigator Benson that he had identified the IP address used in the online conversation and it was registered in Clearwater County, Minnesota. (Id.). After drafting an administrative subpoena for the information, Investigator Benson learned from the telephone company with which the IP address was registered that the subscriber was named Robert Granley. (Id.). The telephone company also provided a physical address for the IP address. When Investigator Benson conducted a Minnesota driver's license check on licenses in the name Michael Granley, he found a Michael Granley with a listed address identical to the physical address for the IP address; this was Defendant. (Id.).

All of this information is included in the affidavit in support of the search warrant, and provides a sufficient base for any statements in the affidavit that identify Defendant as being associated with the online conversation with the girl in Virginia. Although the affidavit does not detail exactly how the Virginia detective obtained the IP address, the Eighth Circuit has

cautioned against hypertechnical review of affidavits for probable cause. See Grant, 490 F.3d at 632. Probable cause is a fluid concept that focuses on factual and practical considerations of everyday life upon which reasonable, prudent men, and not legal technicians, rely to act. Colbert, 605 F.3d at 576. Courts use a totality of the circumstances test to determine probable cause. Hager, 710 F.3d at 836. Under the totality of the circumstances presented here, the lack of information about how the Virginia detective obtained the IP address is not fatal to the probable cause determination, nor is the connection of Defendant with the IP address a conclusory statement.

Defendant also challenges the initial warrant on the ground that the affidavit lacked the sufficient nexus between the evidence sought and the person or property to be searched. (Def. Mem. in Support of Motion to Suppress, [Docket No. 40], 4, 7-8). He asserts that the affidavit fails to provide evidence that he even had a cell phone, tablet, or computer, or to provide "any information associated [*sic*] him with the use of any such devices." (Id.). The information in the affidavit belies this assertion as well.

"[T]here must be evidence of a nexus between the contraband and the place to be searched before a warrant may properly issue." United States v. Tellez, 217 F.3d 547, 550 (8th Cir. 2000). However, it is also well understood that a court issuing a search warrant may draw reasonable inferences from the totality of the circumstances in making its probable cause determination. See Technical Ordnance, Inc. v. United States, 244 F.3d 641, 647 (8th Cir. 2001). As stated above, the affidavit in support of the first search warrant explained how Investigator Benson came to identify Defendant as a person associated with a sexually charged online conversation with a 12-year-old girl. Because the conversation was online, it would have been reasonable for the issuing court to infer that Defendant used a computer, tablet, or cell phone to

facilitate the conversation. Considering the nature of the conversation, it would have also been reasonable to infer that such devices could contain evidence of a crime. For these reasons, the Court finds unpersuasive Defendant's argument that the affidavit did not show a sufficient nexus between the evidence sought and the person or property to be searched.

In addition, Defendant contends that the affidavit is insufficient because it fails to specify the crime allegedly committed. (Def. Mem. in Support of Motion to Suppress, [Docket No. 40], 6). The Eighth Circuit has explicitly held, however, that "[i]t is not necessary for an affidavit to include the name of the specific crime alleged. Rather, '"only a *probability* of criminal conduct need be shown."'" United States v. Summage, 481 F.3d 1075, 1078 (8th Cir. 2007) (citations omitted). Although Investigator Benson's affidavit in support of the initial search warrant application did not specifically name a crime, the factual allegations in the affidavit support a finding that there was probable cause to believe that Defendant had engaged in a crime. For example, Defendant's request that J.G. send him a picture of her breasts supports a finding of probable cause that Defendant was committing the crime of production of child pornography, in violation of 18 U.S.C. § 2251(a), which prohibits "persuad[ing] . . . any minor to engage in . . . any sexually explicit conduct for the purpose of producing any visual depiction of such conduct," or electronic solicitation of children to engage in sexual conduct, in violation of Minn. Stat. § 609.352(2a).[3]

Next, Defendant argues that the affidavit is insufficient because it does not specify dates for the reports from Virginia and Bemidji or for the activities alleged in those reports. (Def. Mem. in Support of Motion to Suppress, [Docket No. 40], 7). He avers that the omission of such

[3] On June 20, 2016, the Court of Appeals of Minnesota held that Minn. Stat. § 609.352(2a)(2) was unconstitutionally overbroad, but at the time Investigator Benson applied for the initial warrant in the case presently before the Court, the statute was still in effect. See State v. Muccio, 881 N.W. 2d 149 (Minn. Ct. App. 2016), rev. granted Aug. 23, 2016.

dates means that the information could be stale because it's possible the conversations could have taken place decades prior to the application for the search warrant, which makes it unreasonable to conclude that there is probable cause that evidence of the activities would still be found at Defendant's home or on his electronic devices. (Id. at 8-9). The Government responds that controlling case law shows that the lack of dates has no impact on the probable cause determination, considering the recognized tendency of child pornography collectors to maintain collections of such pornography. (Govt. Response, [Docket No. 42], 17-18). In addition, the Government contends that the affidavit showed that Defendant's crimes were ongoing, so the time between the original events and the warrant application becomes less important. (Id. at 18-19).

"The date of the occurrence of the facts relied upon in an affidavit is of importance in the determination of probable cause because untimely information may be deemed stale." Summage, 481 F.3d at 1078 (citations omitted). "Given the compulsive nature of the crime of possession of child pornography and the well-established hoarding habits of child pornography collectors, there is no 'bright-line' test for determining when information is stale or the probative value of all suspected child pornography activities." United State v. Notman, 831 F.3d 1084, 1088 (8th Cir. 2016).

Although the affidavit does not contain the dates of the reports or the dates of the occurrences described therein, the affidavit presently at issue did contain facts that showed that Defendant had attempted to obtain a photograph of a 12-year-old girl's breasts and genitals. It also established that Defendant had at least one other conversation in which he alluded to sexual activity with another 12-year-old girl. This information was sufficient to support a reasonable inference that Defendant was engaged in an ongoing effort to obtain child pornography, which

supports a reasonable conclusion that there was probable cause to believe that such images would be found in Defendant's home, on his person, or stored in his electronic devices. See United States v. Colbert, 605 F.3d 573, 578 (8th Cir. 2010) ("Computers and internet connections have been characterized . . . as tools of the trade for those who sexually prey on children."); United States v. Estey, 595 F.3d 836, 840 (8th Cir. 2010) (recognizing that the Eighth Circuit, and others, have held that evidence developed within several months of an application for a search warrant for a child pornography collection and related evidence is not stale."); United States v. Lemon, No. 8-cr-246 (DSD/SRN), 2008 WL 4999235, *2 (D. Minn. Nov. 19, 2008) ("Individuals who seek sexual gratification involving children often store images of child pornography on their computers, often for months or years.").

Here, the affidavit begins by stating that Investigator Benson reviewed the report from Virginia on January 14, 2016. (Govt. Exh. 3, [Docket No. 34-3], 4). Thereafter, Investigator Benson spoke with local law enforcement, who informed him about the IP address used in the online conversation. (Id.). After learning the physical address associated with the IP address, Investigator Benson identified Defendant as associated with that physical address. The chronological nature of the affidavit's narrative and the date on which that narrative begins support a reasonable inference that there was probable cause to believe evidence of a crime would be found at Defendant's home or on his person. Therefore, although the dates of the prior conversations could have strengthened support for a probable cause finding resulting from this affidavit, the lack of such dates is not fatal under the totality of the circumstances and nature of the case now before the Court.

b. Authorization for the search and seizure of the Cell Phone and Tablet

Defendant briefly argues that because the initial search warrant only authorized the search of his home and person, it did not authorize the search and seizure of the iPhone or tablet because those items were seized by Investigator Benson at the real estate office. (Def. Mem. in Support of Motion to Suppress, [Docket No. 40], 9). As the Government points out, however, Investigator Benson testified at the motions hearing that Defendant had his iPhone on his person when he gave it to Investigator Benson. (Motions Hearing, September 30, 2016, Digital Record, 2:09-:11, 2:20-21). Similarly, Defendant voluntarily retrieved his tablet and gave it to Investigator Benson. (Id.). These facts support a finding that the tablet and iPhone were taken from Defendant's person. See United States v. Rolla, No. 07-cr-222 (DWF/JJG), 2007 WL 3243942, *2-3 (D. Minn. Nov. 1, 2007) (finding the defendant's wallet "was taken from [the defendant] personally" where, although officer "was not absolutely certain about where the wallet was recovered, he stated that [the defendant] handed the wallet over.").

c. Particularity and scope

Next, Defendant argues that the affidavit was insufficient because it did not provide probable cause to justify the search of the contents of the iPhone and tablet; he claims that the warrant was unconstitutionally general, containing no limitations and authorizing an unconstitutionally broad search. (Def.'s Mem. in Support of Motion to Suppress, [Docket No. 40], 10-15). In response, the Government argues that the warrant was sufficiently particular in identifying the cell phone and tablet and provided adequate information to support a determination that there was probable cause to search those items. (Govt.'s Response, [Docket No. 42], 12-17).

Defendant cites Riley v. California, 134 S. Ct. 2473, 2485 (2014), the United States Supreme Court addressed the permissibility of warrantless searches of data on cell phones incident to a lawful arrest, ultimately holding "that officers must generally secure a warrant before conducting such a search." In doing so, the Court noted that "[c]ell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person," in part because of their immense storage capacity. 134 S. Ct. at 2489-91. Because Riley addressed *warrantless* searches of cell phone data, it is not controlling here, where officers obtained a search warrant prior to searching Defendant's cell phone and tablet.

Defendant also analogizes the current case to United States v. Winn, 79 F. Supp. 3d 904 (S.D. Ill. 2015). (Def.'s Mem. in Support of Motion to Suppress, [Docket No. 40], 13-4). In Winn, as part of an investigation into a report that a man had used his cell phone to photograph or videotape underage girls without their permission at a public pool, Nathaniel Winn consented to police seizure of his cell phone. 79 F. Supp. 3d at 909-10. An officer later applied for a warrant to search the cell phone for

> any or all files contained on said cell phone and its SIM Card or SD Card to include but not limited to the calendar, phonebook, contacts, SMS messages, MMS messages, emails, pictures, videos, images, ringtones, audio files, all call logs, installed application data, GPS information, WIFI information, internet history and usage, any system files on phone, SIM Card, or SD Card, or any data contained in the cell phone, SIM Card or SD Card to include deleted space.

Id. at 911.

A state court Circuit Judge signed the search warrant, and the search of the cell phone revealed pornographic images of children. Id. After Winn was indicted for receipt of visual depictions of minors engaged in sexually explicit conduct, he moved to suppress the evidence obtained from his cell phone for multiple reasons, including that the search warrant was overbroad and lacked sufficient particularity. Id. at 912. Winn argued that the broad scope of the

search warrant "essentially invited the police to conduct an illegal general search of his cell phone." Id. On appeal, the United States District Court for the Southern District of Illinois agreed.

Noting that the Seventh Circuit has instructed police officers to narrowly tailor warrants, the Winn court held that "[w]ith regard to the objects of the search, . . . the warrant was facially overbroad, exceeded the probable cause to support it, and was not as particular as the circumstances would allow" because "the police did not have probable cause to believe that *everything* on the phone was evidence of the crime" being investigated. Id. at 919. The court noted that the affidavit contained no basis to believe that data other than photos and videos could possibly be evidence of the crime; therefore, the court concluded, that "the warrant was overbroad, because it allowed the police to search for and seize broad swaths of data without probable cause to believe it constituted evidence of [the crime identified in the warrant application]." Id. at 920.

Here, Defendant urges this Court to adopt the Seventh Circuit's reasoning in Winn. (Def.'s Mem. in Support of Motion to Suppress, [Docket No. 40], 14-15). He asserts that the affidavit contained "no information that either the [cell] phone or tablet contained evidence of a crime" and, therefore, there was no probable cause to support the search of the iPhone and tablet. (Id. at 14-15). The Court disagrees.

As explained above, upon review of Investigator Benson's affidavit, the Court finds that the issuing state court judge had a sufficient basis upon which to believe that probable cause existed for the issuance of the search warrant for Defendant's cell phone and tablet. The affidavit includes information showing that the multi-state investigation had determined that the potential crimes of production of child pornography or electronic solicitation of children to engage in

sexual conduct being committed were facilitated, in large part at least, by use of the internet. Thus, it was reasonable for the issuing judge to conclude that there was a fair probability that evidence of that criminal activity would be found in a cell phone or tablet, both of which are plainly capable of accessing the internet. The affidavit articulates a sufficient basis upon which to find that a fair probability existed to conclude that the search would uncover evidence of a crime; thus, there was probable cause to issue the warrant to search Defendant's cell phone and tablet.

To the extent that Defendant is raising a particularity argument about the initial warrant itself, the Fourth Amendment requires warrants to "particularly describ[e] the place to be searched, and the person or things to be seized." U.S. Const. Amend. IV. Defendant briefly contends that because "neither the specific cell phone or tablet taken . . . are specified in the warrant application," their seizure and search were impermissible. (Def. Mem. in Support of Motion to Suppress, [Docket No. 40], 10).

> Particularity prohibits the government from conducting "general, exploratory rummaging of a person's belongings." "To satisfy the particularity requirement of the fourth amendment, the warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized." Furthermore, "[t]he degree of specificity required will depend on the circumstances of the case and on the type of items involved." This particularity standard is one of "practical accuracy rather than" of hypertechnicality.

United States v. Sigillito, 759 F.3d 913, 923 (8th Cir. 2014).

As set forth above, the warrant authorized the search and seizure of "personal electronic devices including, but not limited to: cell phones, personal data assistants, portable audio devices, digital cameras, digital video recorders, video entertainment consoles, and/or any other data storage medium." (Govt. Exh. 3, [Docket No. 34-3], 6). At the time Investigator Benson applied for the warrant, he knew that the suspect conversations had occurred online; he did not

know the specific device used to access the internet and participate in the conversations. Therefore, it was necessary to search a broader spectrum of electronic devices available to Defendant that could be used to facilitate the online communication. In addition, because the male participant in these conversations requested pictures of J.G.'s breasts, it was necessary to search a broad spectrum of devices that could store visual media such as photographs. Under the totality of the circumstances of this case, the Court concludes that the warrant was not overbroad nor did it lack in particularity.

d. Leon Good-Faith Exception

In addition, assuming solely for the sake of argument that the affidavit in support of the initial warrant was not sufficient to establish probable cause, the Court concludes that officers relied in good faith on the probable cause determination by the state court judge when executing the initial search warrant.

Although evidence obtained as a result of the execution of a warrant unsupported by probable cause is generally inadmissible, Mapp v. Ohio, 367 U.S. 643 (1961), there is an exception "when the police conduct a search in 'objectively reasonable reliance' on a warrant later held invalid." Davis v. United States, 564 U.S. 229, 238-39 (2011) (quoting United States v. Leon, 468 U.S. 897, 922 (1984)). There are four circumstances in which the good-faith exception does not apply:

> (1) the magistrate judge issuing the warrant was misled by statements made by the affiant that were false or made "in reckless disregard for the truth"; (2) "the issuing magistrate judge wholly abandoned his [or her] judicial role"; (3) the affidavit in support of the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) the warrant is "so facially deficient . . . that the executing officers cannot reasonably presume it to be valid.

United States v. Marion, 238 F.3d 965, 969 (2001). Here, Defendant contends that the latter two circumstances apply. (Def.'s Mem. in Support of Motion to Suppress, [Docket No. 40], 15-17). Again, the Court disagrees.

The record currently before the Court shows that law enforcement's good-faith reliance on the warrant issued to search Defendant's cell phone and tablet militates against suppressing the evidence obtained during the search. In his affidavit in support of his application for the initial search warrant, Investigator Benson presented specific facts indicating that Defendant had engaged in sexually inappropriate online conversations with two 12-year-old girls. The affidavit related Investigator Benson's understanding that "an electronic device connected to the internet via wireless or hard wire is needed to access and maintain the Facrbook page" and asked for a search warrant in order to "access the electronic devices maintained and/or utilized by [Defendant] for the purpose of maintaining and/or collecting of photographs of children for either personal gratification or trade." (Govt. Exh. 3, [Docket No. 34-3], 5). Accordingly, the affidavit in support of the warrant was not "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." In addition, although the scope of the search was somewhat broader, it did not render the warrant "so facially deficient . . . that the executing officers cannot reasonably presume it to be valid."

Thus, the Court concludes that the officers involved in seizing and searching Defendant's cell phone and tablet relied in good faith on the search warrant which had been issued by state court Judge Melbye based on the application for a warrant setting forth those facts.

Because the Court finds that the issuing judge had a substantial basis upon which to conclude that probable cause existed for the issuance of the initial search warrant for the contents

of Defendant's cell phone and tablet, the Court recommends that Defendant's Motion to Suppress Evidence Obtained as a Result of Search and Seizure, [Docket No. 31], be **DENIED**. [4]

III. CONCLUSION

Based on the foregoing, and all the files, records, and proceedings herein, **IT IS HEREBY RECOMMENDED** that:

1. Defendant's Motion to Suppress, [Docket No. 31], be **DENIED**.

Dated: November 2, 2016

s/Leo I. Brisbois
The Honorable Leo I. Brisbois
United States Magistrate Judge

N O T I C E

Filing Objections: This Report and Recommendation is not an order or judgment of the District Court and is therefore not appealable directly to the Eighth Circuit Court of Appeals.

Under Local Rule 72.2(b)(1), "A party may file and serve specific written objections to a magistrate judge's proposed findings and recommendation within 14 days after being served with a copy of the recommended disposition[.]" A party may respond to those objections within 14 days after being served a copy of the objections. LR 72.2(b)(2). All objections and responses must comply with the word or line limits set forth in LR 72.2(c).

Under Advisement Date: This Report and Recommendation will be considered under advisement 14 days from the date of its filing. If timely objections are filed, this Report and Recommendation will be considered under advisement from the earlier of: (1) 14 days after the objections are filed; or (2) from the date a timely response is filed.

[4] Defendant also argues that because the initial search warrant was fatally defective, the use of the information discovered through the first search warrant could not properly be used in subsequent applications for additional search warrants. (Def.'s Mem. in Support of Motion to Suppress, [Docket No. 40], 15). Defendant asserts that once this information is removed from the later search warrant applications, those applications lack probable cause to support the resulting search warrants, so the Court should suppress any information gleaned from the later searches. Because the Court finds that the initial search warrant was not unconstitutional, the Court need not address these derivative "fruit of the poisonous tree" arguments.